REMARKS

Claims 13, 16, and 21 to 24 have been amended above. New claims 25 to 31 have been added. No new matter has been added. Claims 13 to 31 are pending. Applicants respectfully request reconsideration of the present application in view of this response.

Specification

The Specification was objected for lack of mention of "data carrier." The Specification has been amended above to correct this matter. Support for the amendment is based on the Specification itself and original claim 11, among other support. No new matter has been added. Applicants respectfully request acceptance of the amendment, and withdrawal of the objection to the Specification.

Objection to Claims

Claim 16 was objected to for an informality regarding the symbol between the 'k' and the 'm' in lines 1 and 2. The symbol is a dot at midlevel range which is commonly used as a multiplication sign. Above, Applicants have presented claim 16 again so that the symbol is clearly viewable. No new matter has been added. Withdrawal of the objection to claim 16 is respectfully requested.

35 U.S.C. § 112, second paragraph

Claim 16 was rejected under 35 U.S.C. § 112, second paragraph, for insufficient antecedent basis. Applicants have corrected this error above, and claim 16 is believed allowable. No new matter has been added. Withdrawal of the rejection of claim 16 is respectfully requested.

35 U.S.C. § 101

Claims 13 to 23 were rejected under 35 U.S.C. § 101 for reciting a process without being associated with a machine. Claims 13, 21, and 22, have been amended above to recite a machine. Claims 14 to 20 depend from claim 13. Claim 23 recites a data carrier which is a storage device or machine. No new matter has been added. Accordingly, Applicants believe that the claims as amended above do recite statutory matter and are believed allowable. Withdrawal of the rejection of claims 13 to 23 is respectfully requested.

35 U.S.C. § 103(a)

Claims 13 to 17 and 20 to 24 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,266,411 to Etzel et al. ("Etzel reference") in view of U.S. Patent No. 6,052,467 to Brands ("Brands reference"), and further in view of "An Identity Based Encryption Scheme Based on Quadratic Residues" by Cocks ("Cocks reference").

The Etzel reference purportedly concerns a multiple-iteration Cellular Message Encryption Algorithm (CMEA) process in which a plaintext message is introduced into the system and subjected to a first iteration of a CMEA process, using a first CMEA key to produce an intermediate ciphertext. Then, according to the reference, the intermediate ciphertext is subjected to a second iteration of the CMEA process using a second CMEA key to produce a final ciphertext. In a further step, the reference refers to subjecting the plaintext and intermediate ciphertext to input and output transformations before and after each iteration of the CMEA process. According to the Etzel reference, the CMEA iterations are performed using an improved use of a tbox function which adds permutations to a message or intermediate crypto-processed data.

The Brands reference purportedly concerns a cryptographic method that enables the issuer in a secret-key certificate issuing protocol to issue triples consisting of a secret key, a corresponding public key, and a secret-key certificate of the issuer on the public key, such that receiving parties can blind the public key and the certificate but not a predetermined non-trivial predicate of the secret key even when executions of the issuing protocol are performed in parallel.

The Cocks reference purportedly concerns an offline public key system in which a user's identity, e.g., email address, is used to allow one to access encrypted data. The Cooks reference paper proceeds to discuss the security deficiencies of its system in that one way to break the system is to factorize a universally available public modulus M, and that their paper study assumes that M has not been factorized.

In contrast, amended claim 13 is directed to a method for encrypting data according to an asymmetrical method using a processor, based on a factorization problem, in which a public key and a private key are provided, the public key being the iteration number L as well as the composite number n; the private key is made up of the factorization of n; the message $m = (m_1, m_2)$ to be encrypted is made up of at least the components m_1 *and* m_2; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n in order to allow for retrieval of the original message from the encrypted information $c = (c1, c2)$. The Etzel reference refers to using CMEA iterations using an improved use of a tbox function which adds permutations to a message or intermediate crypto-processed data. Claim 13 is directed to its own factorization and encryption method, i.e., specific quadratic relationships as claimed. The Brands

reference also does not teach or describe the invention as claimed in claim 13. The Brands reference concerns blinding the public key, and does not teach or describe the specific quadratic relationships as claimed. The Cocks reference, in fact, teaches away from the present invention in that it does not intend to deal with the factorization problem in a practical manner and, thus, is not properly combinable with and does not cure the deficiencies of the Etzel and Brand references.

Accordingly, amended claim 13 is believed allowable and withdrawal of the rejection is respectfully requested.

The remaining claims either recite features analogous to amended claim 13 or depend from amended claim 13, and are believed allowable for essentially the same reasons. Withdrawal of the rejection of claims 13 to 17 and 20 to 24 is respectfully requested.

Claims 18 and 19 were rejected under 35 U.S.C. § 103(a) as unpatentable over the Etzel reference in view of the Brands reference and further in view of the Cocks reference and further in view of U.S. Patent No. 6,792,108 to Patera et al. ("Patera reference").

Claims 18 and 19 depend from claim 13 and are believed allowable over the Etzel, Brands, and Cocks references for the same reasons. The Patera reference does not cure the deficiencies of those references.

The Patera reference purportedly concerns a sequence generator using a quasi-crystal function to prepare an encryption or decryption pad. Specifically, the Patera reference refers to techniques for generating purely aperiodic sequences using quasi-crystal functions. In constrast to claims 18 and 19 which depend from claim 13, the Patera does not teach or describe the specific quadratic relationships claimed. Accordingly, claims 18 and 19 are believed allowable. Withdrawal of the rejection of claims 18 and 19 is respectfully requested.

Applicant respectfully believes that claims 13 to 24, as now amended, and new claims 25 to 31, are in condition for allowance.

CONCLUSION

In view of the foregoing amendment and remarks, it is believed that the objections to the Specification and claims have been overcome, and that the rejections of the claims have been obviated, and that pending claims 13 to 31 are allowable. It is therefore respectfully requested that the objections and rejections be withdrawn, and that the present application issue as early as possible.

Applicants readily welcome telephonic contact with the Examiner in an effort to further the present application towards allowance and issuance.

Respectfully submitted,

Dated: October 1, 2009

By: _/Linda Lecomte/_____
Linda Shudy Lecomte (Reg. No. 47,084)
KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200
CUSTOMER NO. 26646